

ABSTRACT

A system and method for determining the source, on a network, of unwanted messages generated by a malicious agent, toward a target device such as a web server. The malicious agent directs one or more computers on a sub network to direct a flood of communications toward the server on a second sub network designed to substantially reduce the ability of the server to respond to other communications. Messages passing through points on a path between the malicious agent computers and the server are monitored for indicia of messages uncharacteristic of normal network communication. The first point along the path that the unwanted messages pass through is identified. A network device at that point is instructed to block portion of communications passing through that point.

20272790.doc